Proc. of the Intl. Conf.on Advances in Computing, Electronics and Communication-- ACEC 2013

ISBN: 978-981-07-7965-8

Intelligent Intrusion Detection Approach for SCADA System Protection

S. L. P Yasakethu and J. Jiang

***Abstract*— In traditional intrusion detection systems (IDS) used for critical infrastructure protection, such as SCADA (Supervisory Control and Data Acquisition) systems, intrusion alerts are analyzed by human analysts (security analysts). They evaluate the alerts and take decisions accordingly. Nevertheless, this is an extremely difficult and time consuming task as the number of alerts generated could be quite large and the environment may also change rapidly. This makes automated detection techniques more efficient for intrusion detection than human analysts. This paper we describes a new European Framework-7 funded research project, CockpicCI, and introduce an intelligent rick detection and analysis technique for Critical Infrastructures (CI). Results show that the proposed OCSVM (One Class Support Vector Machine) based intrusion detection approach can be effectively used to detect both known and unknown attacks.**

Keywords*— Critical infrastructures, Anomaly detection and Cyber-security.

I. Introduction

Industrial Control Systems (ICS) are command and control networks and systems designed to support industrial processes. These systems are responsible for monitoring and controlling a variety of processes and operations such as gas and electricity distribution, water treatment, oil refining, railway transportation, etc. The largest subgroup of ICS is SCADA systems. In the last few years, ICS have passed through a significant transformation from proprietary, isolated systems to open architectures and standard technologies highly interconnected with other corporate networks and the Internet. Today, ICS products are mostly based on standard embedded systems platforms, applied in various devices, such as routers or cable modems, and they often use commercial off-the-shelf software. All this has led to cost reductions, ease of use and enabled the remote control and monitoring from various locations. However, an important drawback derived from the connection to intranets and open communication networks, is the increased vulnerability to cyber-attacks.

S. L. P. Yasakethu *(Author)*
Department of Computing, University of Surrey, Guildford, Surrey, GU2 7XH, UK.

J. Jiang *(Author)*
Department of Computing, University of Surrey, Guildford, Surrey, GU2 7XH, UK.

The protection of the national infrastructures from cyber-attacks is one of the main issues for national and international security. The newly funded European Framework-7 (FP7) research project CockpitCI will introduce intelligent intrusion detection, analysis and protection techniques for Critical Infrastructures (CI). The paradox is that CIs massively rely on the newest interconnected and vulnerable, Information and Communication Technology (ICT), whilst the control equipment, legacy software/hardware, is typically old. Such a combination of factors may lead to very dangerous situations, exposing systems to a wide variety of attacks. To overcome such threats, the CockpitCI project combines machine learning techniques with ICT technologies to produce advance intrusion detection, analysis and reaction tools to provide intelligence to field equipment. This will allow the field equipment to perform local decisions in order to self-identify and self-react to abnormal situations introduced by cyber-attacks.

The CockpitCI System will represent a first step in the synthesis between global awareness and local decision-making capability. Starting from the results of FP7 MICIE [1] project, CockpitCI will aim to define and implement an online distributed risk predictor, able to collect and share information among different infrastructures in real time and predict the evolution of the system. Moreover, the tool will have the ability to detect critical situations such as cyber-attacks, and in case, enable the local decision making capability of smart field equipment, such as RTUs (Remote Terminal Units). The identification of such a methodology and tools will make leverage on previous expertise gained in several EU projects (i.e. SAFEGUARD [2], IRRIIS [3] and MICIE [1]) in the field of CI protection. Moreover, due to the continuous evolution of cyber-attacks and their technological targets, such identification will be tuned by an overview of modelling, methods, techniques, software tools able to represent ICT networks under cyber-attacks with special focus on SCADA systems. With the developments of the above techniques and tools CockpitCI will be able to: a) Deploy smart detection agents to monitor the potential cyber threats according to the types of ICT based networks (e.g. SCADA) and types of devices that belong to such networks. b) Transmit alert to the central CockpitCI centre belonged to the CI owner. c) Analyse the threat, and perform simulation to predict cyber risk level and quality of service (QoS) level for the whole CI.

Rest of the paper will be organized as follows: Section II gives an insight to emerging challengers in cyber-security. CockpitCI detection approach is discussed in section III. Finally section IV concludes the paper.

Proc. of the Intl. Conf.on Advances in Computing, Electronics and Communication-- ACEC 2013

ISBN: 978-981-07-7965-8

II. Emerging challengers in cyber security

Cyber security is a vast topic which includes number of different types of cyber threats, for instance cyber-crime, critical infrastructure protection, cyber terrorism and cyber war among which the term Cyber terrorism is an used to describe an attack from simple hacking to fatal cyber incidents resulting in dangerous financial damage and even physical violence. Recently, global internet security is being one of the most discussed topics as cyber security issues could destroy the countries and their critical infrastructures. National security operatives are alarmed more about the cyber-security issues than physical terrorist attack which could be identified and interrupted with much ease. Terrorist information sharing between the countries has made it harder for terrorists to migrate between countries to carry out physical attacks. Moreover, improvements in spying have facilitated security and anti-terrorism agencies to identify and prevent terrorism plans whereas identity of cyber-terrorists remain unknown and recognizing their physical location remains a major technical challenge.

Critical infrastructures such as electrical power systems are an important part in the day to day life and therefore are in increased threat of being attacked. A successful terrorist attempt to disrupt electricity supplies could have devastating effects on national security, the economy, and every citizen's life. However, power systems are widely spread where that can never be absolutely defended against a determined attack.

Parties that are interested in attacking control systems include terrorists, state-sponsored hackers and even computer geeks who experiment their capabilities. Impact from such an attack could be substantial depending on the political and social importance of the system. Public health, energy production and telecommunication are among the sectors exposed to serious risks that have to be protected at any level as described in an efficient cyber strategy.

With the recent improvement and availability of IT services to the general public hackers increasingly targeted critical infrastructures of numerous occasions. European Network and Information Security Agency's Industrial Control Systems-Cyber Emergency Response Team (ICS-CERT) countered 198 cyber-incidents against critical infrastructures in 2012 which was an increase of 52% compared to 2011. Energy sector was the most suffered in 2012 with a 41% of reported events while water system follows with 15% [4].

CockpitCI will focus on cyber-attacks to control systems of electrical grids that are typically interconnected with public Telco networks. When considering the electrical sector three different types of threats can be identified:

1. Attacks targeting the electrical infrastructure: such attacks are carried out with the intention of creating an outage of supply to the customers. The point of attack could be a single component such as a substation or transmission tower or there could be multiple attacks which intend to bring down an entire regional grid.

2. Attacks which use electrical infrastructure as a weapon: here the ultimate target is the population who uses the supply. Terrorists could use the infrastructure such as cooling towers to disperse chemical or biological agents.

3. Attacks targeting public infrastructure powered by the electrical power: terrorists could use the utility networks as a conduit such as power lines, tunnels, underground cables and sewers to transmit the attacks. For example, terrorists could use the power lines transmit an electromagnetic pulse which would damage the computer systems.

There are two main problems that need to be addressed to defend the critical infrastructures successfully against cyber-attacks:

- Government commitment and awareness: The concept of possibility of a cyber-attack has been considered to be a fiction until the Stuxnet virus which targeted Bushehr nuclear power plant in Iran. This has changed the governments' perception of the cyber offences and the importance of defining an efficient cyber strategy

- Knowledge necessary for a cyber-attack: In contrast the belief that SCADA systems are more vulnerable to attacks, there are several techniques that could lead to a compromised control system such as absence of defense system, improper configurations, zero-day vulnerabilities and superficial patch management process which benefit the mission of the attacker. The main problem is that any professional with no particular knowledge could collect information on a target and how to breach the security easily over the internet.

Below given are several factors that contribute to the increasing susceptibility of control systems:

1) The integration of control systems: organizations have increased connectivity with the integration of their control systems and enterprise networks. Lack of security controls in both networks could cause the breach of enterprise security.

2) Insecure remote connections: use of access links such as dial-up modems and wireless communications are for remote diagnostics, maintenance, and examination of system status. Lack of proper encryption or authentication mechanisms could lead to integrity of information being compromised

3) Standardized technologies: although the standardization could reduce costs and improve system performance, it increases the systems' vulnerability to attacks as more people are armed with knowledge and tools to attack the system.

4) Availability of technical information: with the increase in use of information sharing via www, information about infrastructures and control systems is readily available to potential hackers and intruders. Availability of design and maintenance documents and technical standards for a critical system can on the internet seriously compromise the overall system security.

Proc. of the Intl. Conf.on Advances in Computing, Electronics and Communication-- ACEC 2013

ISBN: 978-981-07-7965-8

III. CockpitCI intrusion detection approach

As discussed earlier, the protection of the national infrastructures from cyber-attacks is one of the main issues for national and international security. To overcome such threats, the CockpitCI project develops machine learning based advance intrusion detection tools to provide intelligence to the field equipment. This will allow the field equipment to perform local decisions in order to self-identify and self-react to abnormal situations introduced by cyber-attacks.

Several techniques and algorithms have been reported by researchers for intrusion detection. One of them is to define the abnormal conditions, however due to the difficulty of defining unknown behaviors these rules based algorithms are always not applicable in the real applications. Generally, anomaly detection can be regarded as a binary classification problem and thus many classification algorithms are utilized for detecting the anomalies, such as artificial neural network [5], support vector machines (SVM) [6], k-nearest neighbor [7] and Hidden Markov model [8]. However, strictly speaking, they are not effective intrusion detection methods, as they require knowing what kind of intrusion is expecting, which deviates from the fundamental object of intrusion detection. Moreover most of these methods are sensitive to noise in the training samples. Segmentation and clustering algorithms [9] seem to be better choices because they do not need to know the signatures of the series. The shortages of such algorithms are that they always need parameters to specify a proper number of segmentation or clusters and the detection procedure has to shift from one state to another state. Negative selection algorithms [10] are designed for one-class classification; however, these algorithms can potentially fail with the increasing diversity of normal set and they are not meant to the problem with a small number of self-samples, or general classification problem where probability distribution plays a crucial role. Furthermore, negative selection only works for a standard sequence, which is not suitable for online detection. Other algorithms, such as time series analysis are also introduced to intrusion detections, and again, they may not be suitable for most of the real application cases.

To minimize the above mention drawbacks, an intelligent approach based on OCSVM [One-Class Support Vector Machine] principles is proposed for intrusion detection in CockpitCI and is described in the following paragraphs.

A. *OCSVM detection mechanism*

Below paragraphs briefly explain the OCSVM detection approach.

Consider a data set with $T = \{x_1, x_2, \cdots, x_l\}$, $x \in R^N$, as shown in Figure 1 for a two dimensional case. The task is to find a function f that takes the value "+1" for most of the vectors in the data set (marked by stars in Figure 1 (a)), and "-1" for the other very small part (circles in Figure 1 (a)). The Strategy for OCSVM is to map the input data into Hilbert space H according to a mapping function $X = \phi(x)$, as shown in Figure 1 (b). Then find a hyper-plane to separate the data from the origin to its maximum margin [11, 12,13].

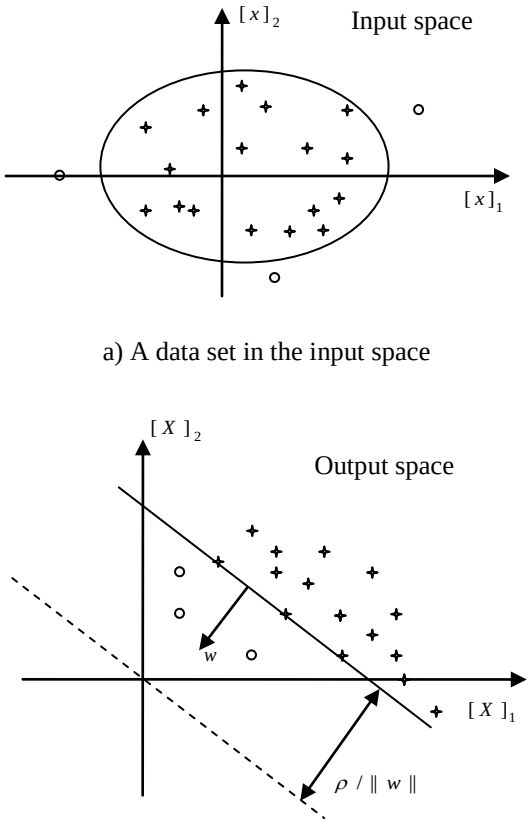

Figure 1. Illustration of the one-class SVM concept

To separate the mapped data from the origin to its maximum is to solve the following quadratic optimisation problem:

$$\min_{w \in F} : \quad \frac{1}{2} \| w \|^2 + \frac{1}{\nu l} \sum_i \xi_i - \rho \qquad (1)$$

$$\text{s.t.} \quad f(x) = w.\phi(x_i) - \rho \geq -\xi_i, \xi_i > 0, \; i = 1, \cdots, l \qquad (2)$$

Where $\nu \in (0,1)$ is the parameter to trade-off between the normal and anomaly data in the data set, that a maximum of $\nu \times 100$ % are expected to return negative values according to $f(x) = w.\phi(x) - \rho$. ξ_i are slack variables acting as penalization in the objective function. Deriving its dual representations, OCSVM is to solve the following problems:

1. Select the kernel function $K(x, x')$ in Hilbert space H, and the trade-off parameter ν, construct and solve the following optimization problem to find the solution

Proc. of the Intl. Conf.on Advances in Computing, Electronics and Communication-- ACEC 2013

ISBN: 978-981-07-7965-8

$\alpha^* = (\alpha_1^*, \cdots, \alpha_l^*)$:

$$\min_{\alpha} : \frac{1}{2}\sum_{i=1}^{l}\sum_{j=1}^{l}\alpha_i\alpha_j K(x_i, x_j) \quad (3)$$

$$\text{s.t.} \quad 0 \le \alpha_i \le 1/(\nu . l), i = 1, \cdots, l \quad (4)$$

$$\sum_{i=1}^{l}\alpha_i = 1 \quad (5)$$

Where $K(x_i, x_j) = \phi(x_i).\phi(x_j)$ is called as kernel function, and can be various format.

2. Select any α^* which satisfied $0 < \alpha^* < 1/(\nu . l)$, and calculate the bias $\rho = \sum_{i}^{l}\alpha_i^* K(x_i, x_j)$, the vectors which satisfied $0 < \alpha^* < 1/(\nu . l)$ are called support vectors.
3. Integrate the decision function $f(x) = \sum_{i=1}^{N_{sv}}\alpha_i^* K(x_i, x) - \rho$, if $f(x) \ge 0$, return +1; otherwise, return the real negative value. N_{sv} is the number of support vectors.

It is proved that $\nu \times 100$ is the upper bound percentage of data that are expected to be outliers in the training data [10], and a vector x_i is detected to be outlier in the training set, if and only if $\alpha_i = 1/(\nu l)$. The parameter directly determines the sensitivity of outlier detection using OSVM. For the testing reported in this paper, we adopt the RBF for the kernel $K(x, y)$ in equation (3), which can be expressed as:

$$K(x, y) = e^{-\|x-y\|^2/(2\sigma^2)} \quad (6)$$

In the algorithm, as discussed above, OCSVM principles are used to train the offline data and generate the detection model, and then the model function is employed for intrusion detection. A negative value returned from the decision function *f(x)* will imply an abnormal event. Flowchart in Figure 2 shows the procedure of the proposed intrusion detection algorithm. For the testing reported in this paper the parameter σ is chosen to be 2.5, and the trade-off parameter ν in equation (4) is selected to be 0.01, which specifies that a maximum of 1% signals in the training set is to be anomaly.

B. *Experiment and results*

We evaluate the performance of the proposed OCSVM based intrusion detection mechanism. KDD Cup 99 intrusion detection data set [14] is used to evaluate the performance of the algorithm. KDD data set utilizes TCP/IP level information and embedded with domain-specific heuristics, to detect

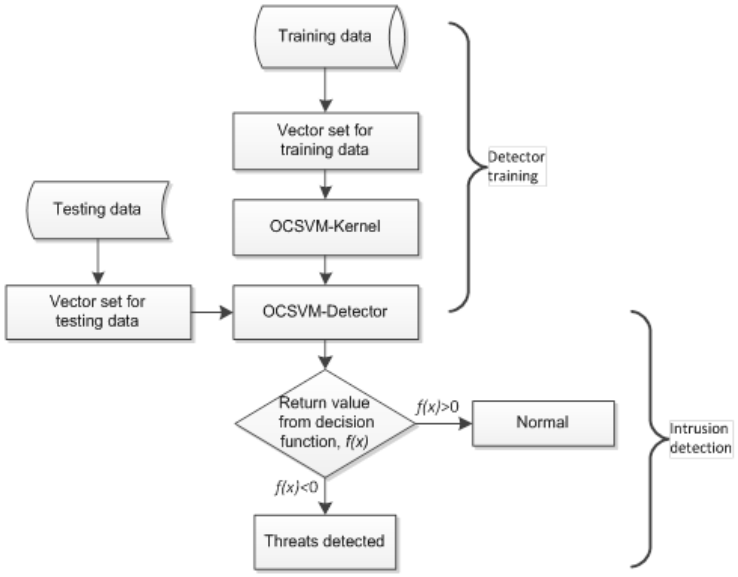

Figure 2: Procedure of the proposed algorithm

intrusions at the network level. The data set contains Normal data plus 24 attack types which are classified into four major categories of attacks, namely Denial of Service (DOS) (attacks which deny legitimate requests to a system), Remote to Local (R2L) (attacks with unauthorized local access from a remote machine), User to Root (U2R) (attacks with unauthorized access to local super-user or root) and Probing (information gathering attacks). Given below are the selected data sets for training and testing phases of the experimental study.

For training, 3-sets of data each having 5000 recodes are selected randomly from the Normal data pool of the KDD data set.

- Training set-A : 5000 Normal data recodes
- Training set-B : 5000 Normal data recodes
- Training set-C : 5000 Normal data recodes

Several tests cases are conducted in order to analyse the performance of the algorithm in detail with respect to specific attack types. Testing data consists of randomly selected normal data and attack data and the composition of the data sets are as follows:

- Testing set-A' : 15000 Normal data recodes + 500 DOS attack data recodes
- Testing set-B' : 15000 Normal data recodes + 500 Probing attack data recodes
- Testing set-C' : 15000 Normal data recodes + 500 R2L attack data recodes
- Testing set-D' : 15000 Normal data recodes + 52 U2R attack data recodes (52 is the maximum no. of U2R attack recodes in the data set)

It should be noted that in all test cases above data is randomly selected for each scenario. The detection accuracy (DA) and false alarm rate (FAR) [15] (FAR is sometimes known as false positive rate) are used as indicators to quantify the performance of the detection mechanism. The detection

Proc. of the Intl. Conf.on Advances in Computing, Electronics and Communication-- ACEC 2013

ISBN: 978-981-07-7965-8

accuracy and the false alarm rate results of the experiments are shown in Table 1. From the tabulated results in Table 1 it is noted that the OCSVM based detection approach shows high detection accuracy and low false alarm rate values for especially for testing data sets with DOS and probing attacks. The detection accuracy and false alarm rate results for testing data with U2R and R2L are also acceptable.

It should be reminded that unlike other machine learning intrusion detection strategies, as explained in section 3, OCSVM approach does not require any label information during the training process. In the case of SCADA performance monitoring, which patterns in data are normal or abnormal may not be obvious to operators. Also, if the detection model relies on signatures of data it is not possible to detect unknown or new attacks. Thus this algorithm can be used to detect previous known as well as unknown (new) attacks real time with high accuracy and a relatively low false alarm rate. As a result, OCSVM based detection model is well suited for intrusion detection in SCADA environment.

IV. Conclusion

The researches performed during the CockpitCI project will allow improving the cyber-security industry. In the real world most of the attacks will remain unknown. Thus, the design and application of real-time intrusion detection methods, which does not require any attack signatures, will be important in developing future CIP and advanced cyber security solutions. Experiments show that OCSVM can effectively detect anomalies and generate alarms, providing excellent potential for further development of practical tools. With the solutions proposed throughout the document CockpitCI will contribute to a safer living environment for people especially by providing smart detection tools, early alerting systems and strategic security system

The authors wish to acknowledge the financial support of the project CockpitCI, funded under European Framework-7 Programme (contract No. 285647).

TABLE 1: PERFORMANCE OF OCSVM BASED DETECTION APPROACH

		Training set-A	Training set-B	Training set-C	Average
Testing set-A'	DA	79.8%	78.9%	80.9%	**79.8%**
	FAR	13%	11%	12%	**12%**
Testing set-B'	DA	76.8%	79.1%	79.2%	**78.37%**
	FAR	10%	11%	11%	**10.67%**
Testing set-C'	DA	73.8%	74.7%	74%	**74.17%**
	FAR	9%	10%	10%	**9.67%**
Testing set-D'	DA	70.3%	70.8%	70.1%	**70.4%**
	FAR	18%	18%	17%	**17.67%**

References

[1] Available at: http://www.micie.eu/index.php
[2] Available at: http://www.safeguardproject.info
[3] Available at: http://www.irriis.org
[4] Available at: http://securityaffairs.co/wordpress/11684/security/scada-and-critical- infrastructures-in-security.html
[5] Gershenson C. Artificial neural networks for beginners. In: Cognitive and computing sciences. University of Sussex.
[6] Christopher. J. C. Burges, A tutorial on support vector machines for pattern recognition, DataMining and Knowledge Discovery, 2(2):955-974, Kluwer Academic Publishers, Boston, 1998.
[7] P. Cunningham and S.J. Delany, k-Nearest Neighbour Classifiers, Technical Report UCD-CSI-2007-4, March 27, 2007.
[8] Rabiner, L. R. (1989). "A tutorial on hidden Markov models and selected applications in speech recognition." Proceedings of the IEEE 77(2): 257-286.
[9] Teknomo, K. (2005), K-Mean Clustering Tutorials. http://people.revoledu.com/kardi/tutorial/kMean/index.html, accessed July 25, 2006.
[10] Zhou Ji, Dipankar Dasgupta, Revisiting Negative Selection Algorithms, Evolutionary Computation, Summer 2007, Vol. 15, No. 2.
[11] M. Lauer. "A mixture approach to novelty detection using training data with outliers". Lecture Notes in Computer Science, pp. 300-310, 2001.
[12] C. Burges. "A tutorial on support vector machines for pattern recognition", Data Mining and Knowledge Discovery(2), pp.121-167, 1998.
[13] B. Schölkopf, R. Williamson et al. "Support vector method for novelty detection", In Neural Information processing Systems, MIT Press, pp 582-588, 2000.
[14] KDD data set, 1999; http://kdd.ics.uci.edu/databases/-kddcup99/kddcup99.html
[15] Available at: http://en.wikipedia.org/wiki/Receiver_operating_characteristic